

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

FR 2 775 812 (Parts)

Date of Application: March 5, 1998
Date of Publication of the Application: September 10, 1999
Applicant: Institut Eurecom Groupement d'intérêt
économique, France

Method for Concealing Binary Information in a Digital Image

Page 1, line 31, through page 3, line 13:

The object of the invention is to suggest a method for concealing a piece of digital information in a document which allows most of the disadvantages of the known methods to be overcome.

More specifically, the object of the invention is to suggest a concealing method which allows hiding information in a still image at gray level, in colors or a video image, or just generally in a multimedia document without visibly degrading the document (or audibly in the case of multimedia audio documents). Particularly in the case of concealing information in images it is important not to degrade the images visually or at least to control the perturbation between predefined terminals a priori.

The object of avoiding perceptible degradation of the document requires that an apparent paradox be solved because, generally, the more one tries to add information to a pre-existing image the more there is a tendency to degrade it, in the sense of its modification.

Another object of the invention is to suggest a robust method for inserting information to be hidden, i.e., in particular such that it is possible to find the hidden information again without the aid of the original documents even after a great number of plausible and non-destructive perturbations of the document.

Another object of the invention is to suggest an open-ended method for concealing information, i.e., that it can be easily corrected so as to remain robust with regard to perturbations of the document which are new or have previously not been taken into account.

For simplification, the following description deals with describing the problems of concealing information in digital images; it is understood, however, that the problem and its

THIS PAGE BLANK (USPTO)

solution extend to any type of multimedia document (image, sound, video,...), according to the invention.

Moreover, in the field of concealing information in images, image protection, the so-called "watermarking", is the most widespread application, but it is understood that the problem solved by the present invention is not limited to such an application since it consists in concealing any type of digital information (not exclusively of the protection type) in a multimedia document. Actually, as will be evident in the following, the particular application of the principle of the invention is principally determined by the characteristics of the information to be concealed.

In order to achieve the objects set, the invention suggests a method for concealing a piece of primary digital information (I_{inf1}) in an initial digital document, in particular an initial multimedia document (I_{orig}), characterized in that it comprises steps consisting in:

- decomposing the initial document (I_{orig}) a priori, by determining a reference digital document (I_{ref}) depending on the initial digital document (I_{orig}) and a piece of secondary digital information (I_{inf2}) depending on the primary digital information to be hidden, such that the sum of the reference digital document (I_{ref}) and said secondary digital information (I_{inf2}) is a modified document (I'_{orig}) substantially equal to the initial digital document (I_{orig});
- inserting the secondary digital information (I_{inf2}) thus determined into said initial document, by calculating a modified image (I'_{orig}) constituted by the sum of said reference digital document (I_{ref}) and said secondary digital information (I_{inf2}), in such a manner as to obtain a modified digital document (I'_{orig}) close to the initial document (I_{orig}), but integrating the primary digital information (I_{inf1}) to be concealed in a substantially indiscernible manner.

Page 4, lines 20 to 30:

- for the extraction from a digital document (I'_{orig}) presumed to be a carrier of a piece of digital information concealed according to the above method, the method comprises steps consisting in:
- calculating a self-similarity code W' associated with the modified image I'_{orig} by using the same context as the one used in the insertion operation;
- retrieving the information I'_{inf2} for each pixel from I'_{orig} and W' by calculating $I'_{inf2} = I'_{orig} - A'$.

THIS PAGE BLANK (USPTO)

- testing the retrieved information $I'_{in\Omega}$ and if $I'_{in\Omega}$ is positive, deducing that the concealed information equals 1; in the contrary case deducing that the concealed information equals 0 for the pixel under consideration, such that the concealed digital information is extracted from the modified digital document (I'_{orig}).

Page 6, line 6, through page 7, line 11:

The initial image to be processed, which will be referred to as I_{orig} , is decomposed into a set of primitives, referred to as "range" or Target, which must cover the entire image (possibly with overlap). Moreover, there is built a basic dictionary $Dbase$, constituted of primitives "domain" or Source. The elements of this dictionary are also extracted (by default) from the image itself, but do not need to cover the entire image to be processed. There is no particular constraint as regards the distribution of the primitives "domain". The dictionary thus built is then enriched by using geometric and photometric transformations to form a final dictionary D_{final} of authorized transformations. It is to be noted that elements may be added to the dictionary D_{final} , kept secret from external users, and be known exclusively by the information insertion/extraction software.

Typically, there will be used transformations of the affine type to create new primitives (however, other, more complex transformations may also be used).

The transformations may include geometric operations (such as an isometry (i.e., symmetries, rotations, reflections), or photometric transformations, for example on the luminance values. In particular, the context permits to define if contractive codes (defined more widely) are used.

It is to be noted that for using the method by means of software, the defined context is indicated to the software in charge of executing the calculations regarding the insertion/extraction of concealed information.

Next, each of the primitives "range" must be paired with a primitive "domain" of the dictionary (see illustration below) according to a distance criterion, for example the minimum distance. In certain cases, by contrast, one might be interested in moving the reference image I_{ref} further away from the initial image I_{orig} so as to (potentially) hide more information across the distance between the two images, pixel by pixel. Usually, the Euclidian distance will be used; however, other distances may be used.

Indexing the primitives "range" by i , w_i designates the transformation it is assigned (i.e., the transformation which defines an element of the basic dictionary, plus one

THIS PAGE BLANK (USPTO)

transformation). W designates the union of the local transformations w_i ; WI the image composed of the entirety of the primitives "range" represented approximately on the basis of an element of D_{final} , and A the attractor associated with W if it exists. It has to be borne in mind in this context that if the selected code is contractive it is possible, by using the Collage theorem, to take into account the attractor A (that is the image obtained by iterating the transformation W n times from any initial image I_{init} : $A = W^n(I_{\text{init}})$), instead of the transformation WI which is the reunion of the blocs "range" approximated from I_{orig} : WI is the transform of I_{orig} through the transformation W applied once: $WI = W(I_{\text{orig}})$.

As a reminder, a given transformation W defines its attractor A because the transformation W applied n times to any image whatsoever yields the image A .

Page 11, line 22, through page 12, line 6:

There will now be described the method of extracting the hidden information I'_{inf2} from a modified image I'_{orig} . This will be done with reference to Figure 2.

In a dual manner to the insertion, the extraction will be realized as follows and as schematically represented in Figure 2.

- Calculating the self-similarity code W' associated with I'_{orig} by using the same context as the one used in the insertion operation; in the indicated step (1'), this yields a reference document designated with I'_{ref} in the general case or with A' in the case of calculating I'_{ref} by means of a fractal method.
- Retrieving I'_{inf2} from I'_{orig} and A' , in the following way:

$$I'_{\text{inf2}} = I'_{\text{orig}} - A'$$

It is to be noted that A' is for I'_{orig} what A was for I_{orig} in the phase of inserting information in I_{orig} . Thus, one tries to reconstruct a reference image A' from the modified image I'_{orig} .

It is to be noted that on the one hand, the IFS codes associated with the images I_{orig} and A are identical (the first one by construction, the second one by defining an attractor), and, on the other, each image point of I'_{orig} is included in the interval defined by its value in I_{orig} and in A .

Blank (USPTO)

Page 15, lines 1 to 29:**INDUSTRIAL APPLICATIONS OF THE INVENTION:**

Numerous applications of this method can already be envisaged now: signature, integrity, non-repudiation, traceability, even error correction and network control points. According to the use aimed at, the presented method may be used unchanged, modulo the definition of an adequate context, to define the type of information to be concealed (i.e., the "design" of the trademark) as well as the parameterization of the insertion and extraction operators. Examples of application will be given below for information purposes.

Signature. This means that an author, a company or the like can protect a document such as an image. This can be done by inserting the company's logo or, for example, the author's face as binary information.

Integrity. This relates to being able to identify whether or not an image has been substantially modified. To this end, the information to be concealed will be linked to characteristics of the image itself: histogram of the gray levels (in the form of a binary image), contour map (in superposition of the image), or a specific motive... There must be noted the following difficulty though: the characteristics of an image will be modified by the very fact of concealing its characteristics in the image itself.

Non-Repudiation. This relates to automatically inserting a trace of the author when he sends an image to a third person: a logo identifying the person (digital imprint, digital signature, ...) and/or the apparatus from which he transmits the image (fax, PC, mobile multimedia terminal,...).

Traceability. The application may be expanded or automated such that one knows, for example by means of a trace, whether or not such-and-such an image has been previously photocopied, printed,....

Network control points: The invention can be used for preventing forbidden images from transiting on networks (like the Internet) by benefiting from simple transformations executed just before automatic control points set up in the network and executed in the reverse direction just afterwards.

THIS PAGE BLANK (USPTO)

① REPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

⑪ N° de publication :

2 775 812

(à n'utiliser que pour les
commandes de reproduction)

⑫ N° d'enregistrement national :

98 04083

⑬ Int Cl⁶ : G 06 T 5/50, H 04 N 5/272

⑭

DEMANDE DE BREVET D'INVENTION

A1

⑮ Date de dépôt : 05 03 98.

⑯ Priorité :

⑰ Date de mise à la disposition du public de la
demande : 10 09 99 Bulletin 99/36.

⑱ Liste des documents cités dans le rapport de
recherche préliminaire : Se reporter à la fin du
présent fascicule.

⑲ Références à d'autres documents nationaux
apparentés :

① Demandeur(s) : INSTITUT EURECOM Groupement
d'intérêt économique — FR.

② Inventeur(s) : DUGELAY JEAN LUC.

③ Titulaire(s) :

④ Mandataire(s) : NONNENMACHER BERNARD.

⑤ PROCÉDE DE DISSIMULATION D'INFORMATIONS BINAIRES DANS UNE IMAGE NUMÉRIQUE.

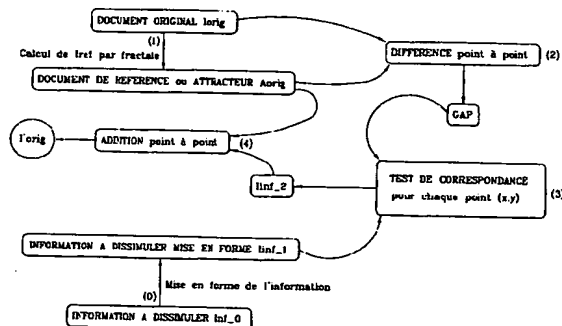
⑥ L'invention concerne un procédé pour dissimuler une
information numérique primaire (I_{inf1}) dans un document numé-
rique initial, notamment un document multimedia initial
(I_{orig}), caractérisé en ce qu'il comporte des étapes consis-
tant à :

- décomposer le document initial (I_{orig}) à priori, en déter-
minant un document numérique de référence (I_{ref}) fonction
du document numérique initial (I_{orig}), notamment par une
méthode fractale et une information numérique secondaire
(I_{inf2}) fonction de l'information numérique primaire à cacher,
tels que la somme du document numérique de référence
(I_{ref}) et de ladite information numérique secondaire (I_{inf2})
soit un document modifié (I_{mod}) sensiblement égale au do-
cument numérique initial (I_{orig});
- insérer l'information numérique secondaire (I_{inf2}) ainsi
déterminée dans ledit document initial, en calculant une ima-
ge modifiée (I_{mod}) constituée par la somme dudit document
numérique de référence (I_{ref}) et de ladite information numé-
rique secondaire (I_{inf2}), de façon à obtenir un document nu-
mérique modifié (I_{mod}) proche du document initial (I_{orig})
mais intégrant de façon sensiblement indiscernable l'informa-
tion numérique primaire (I_{inf1}) à dissimuler.

Le procédé selon l'invention permet de façon duale,
d'extraire l'information numérique cachée dans un docu-

ment multimédia.

Le procédé selon l'invention, basée sur la notion d'auto-
similarité, permet, sous certaines conditions, que l'informa-
tion introduite ne soit pas visible, résiste à des manipula-
tions de l'image, et enfin puisse être extraite sans
connaissance des documents originaux.



FR 2 775 812 - A1



La présente invention concerne un procédé permettant de cacher une information numérique dans un document numérique multimedia, (par exemple le logo d'une société dans une image en niveaux de gris émise par la société), puis de retrouver à partir du document modifié, l'information préalablement dissimulée. L'invention concerne également l'utilisation de ce procédé dans diverses applications pouvant tirer avantage du procédé de dissimulation d'information dans une image numérique.

ETAT DE LA TECHNIQUE

Il existe déjà une pluralité de techniques consistant à cacher une information numérique dans une image, et ce pour des applications principalement de type « watermarking » en terminologie anglosaxonne, consistant à marquer des documents numériques pour pouvoir prouver leur originalité.

Il existe par ailleurs des techniques d'encryptage. Cependant les techniques d'encryptage ont le plus souvent pour objectif et pour résultat que le document encrypté est totalement illisible, ce qui écarte ce type de technique du champ de la présente invention, dans laquelle on cherche dans certaines applications à sécuriser un document tout en préservant sa bonne lisibilité.

De façon générale, toutes les techniques de dissimulation d'information dans une image connues à ce jour comportent un ou plusieurs inconvénients, parmi les suivants:

- elles dégradent l'image visuellement et de manière mal contrôlée;
- elles manquent de robustesse vis à vis de transformations de base de l'image, ce qui empêche l'extraction fiable de l'information qu'on a voulu y cacher;
- certaines techniques nécessitent le recours à l'image originale pour pouvoir extraire l'information, donc l'image modifiée par dissimulation d'informations ne s'autosuffit pas pour retrouver l'information cachée.

BUTS DE L'INVENTION:

L'invention a pour but de proposer un procédé de dissimulation d'une information numérique dans un document, permettant de résoudre la plupart des inconvénients des

procédés connus.

Plus spécifiquement, l'invention a pour but de proposer un procédé de dissimulation permettant de cacher de l'information dans une image fixe en niveaux de gris, en couleurs ou une image dans une vidéo, ou de façon tout à fait générale dans un document multimédia, sans dégrader le document de façon perceptible (ou audible, dans le cas de document
5 multimédia audio). En particulier, dans le cas de dissimulation d'information dans des images, il est important de ne pas dégrader les images visuellement, ou du moins de contrôler à priori la perturbation entre des bornes prédéfinies.

Le but visant à éviter des dégradations perceptibles du document nécessite de
10 résoudre un paradoxe apparent car en général, plus on essaie de rajouter de l'information à une image pré-existante, plus on aura tendance à la dégrader, au sens de sa modification.

Un autre but de l'invention est de proposer un processus d'insertion de l'information à cacher qui soit robuste, c'est-à-dire en particulier tel que même après un grand nombre de perturbations plausibles et non destructives du document, il soit possible de retrouver
15 l'information cachée, sans l'aide des documents originaux.

Un autre but de l'invention est de proposer un procédé de dissimulation d'information qui soit évolutif, c'est-à-dire qu'il puisse être aisément corrigé pour rester robuste vis-à-vis de perturbations du document nouvelles ou non prises en compte précédemment.

20 Dans la suite de la description, on s'attachera pour simplifier à décrire la problématique de la dissimulation d'information dans des images numériques, étant entendu que le problème et sa solution sont étendus, selon l'invention, à tout type de document multimédia (image, son, vidéo, ...).

En outre, dans le domaine de la dissimulation d'informations dans des images, la
25 sécurisation d'image, dite « watermarking », est l'utilisation la plus répandue, mais il doit être bien compris que le problème résolu par la présente invention n'est pas limité à une telle utilisation, puisqu'il consiste à dissimuler une information numérique de type quelconque (non exclusivement sécuritaire) dans un document multimédia. En fait, comme cela apparaîtra dans la suite, l'utilisation particulière du principe de l'invention sera déterminée
30 principalement par des caractéristiques de l'information à dissimuler elle-même.

Afin d'atteindre les buts fixés, l'invention propose un procédé pour dissimuler une information numérique primaire (I_{inf1}) dans un document numérique initial, notamment un

document multimedia initial (I_{orig}), caractérisé en ce qu'il comporte des étapes consistant à:

- décomposer à priori le document initial (I_{orig}), en déterminant un document numérique de référence (I_{ref}) fonction du document numérique initial (I_{orig}), et une information numérique secondaire (I_{inf2}) fonction de l'information numérique primaire à cacher, tels que la somme du document numérique de référence (I_{ref}) et de ladite information numérique secondaire (I_{inf2}) soit un document modifié (I'_{orig}) sensiblement égal au document numérique initial (I_{orig});

- insérer l'information numérique secondaire (I_{inf2}) ainsi déterminée dans ledit document initial, en calculant une image modifiée (I'_{orig}) constituée par la somme dudit document numérique de référence (I_{ref}) et de ladite information numérique secondaire (I_{inf2}), de façon à obtenir un document numérique modifié (I'_{orig}) proche du document initial (I_{orig}) mais intégrant de façon sensiblement indiscernable l'information numérique primaire (I_{inf1}) à dissimuler.

Selon d'autres caractéristiques du procédé de l'invention:

- plus précisément, la valeur de chaque pixel du document modifié (I'_{orig}) est comprise entre (ou égale à, ou comprise entre, ou plus généralement repérée par rapport à) sa valeur calculée dans le document numérique de référence (I_{ref}) et sa valeur donnée dans le document initial (I_{orig});

- Pour déterminer le document numérique de référence (I_{ref}) à partir du document initial (I_{orig}), on utilise la méthode des fractales, consistant à:

- découper le document initial (I_{orig}) en un ensemble de primitives RANGE(i) couvrant la totalité du document initial;
- extraire du document initial (I_{orig}) un ensemble de primitives DOMAIN(i), de façon à constituer un dictionnaire de primitives DOMAIN(i) de base (Dbase);
- à partir du dictionnaire de primitives DOMAIN de base, déterminer un dictionnaire (Dfinal) de primitives DOMAIN supplémentaires, en appliquant aux primitives de base, un ensemble de transformations géométriques et/ou photométriques locales;
- appairer chacune des primitives de base RANGE(i) avec une primitive DOMAIN(i) du dictionnaire de primitives (Dbase), de telle manière que chaque primitive RANGE(i) soit égale à la transformée d'une primitive DOMAIN(i) par une transformation élémentaire w_i , plus une erreur (ϵ_i), ladite erreur permettant de dissimuler l'information numérique à cacher (I_{inf1}), l'image composée de l'ensemble des primitives RANGE calculées à partir d'une

primitive DOMAIN du dictionnaire (Dfinal) étant notée WI_{orig} (ou A dans les circonstances expliquées plus loin);

- de préférence, pour déterminer l'information numérique secondaire à cacher ($I_{in\Omega}$) à partir de l'information numérique primaire à cacher ($I_{in\Gamma}$), on calcule la différence $GAP = I_{orig} - WI_{orig}$ (ou A pour un code contractif) entre le document initial (I_{orig}) et l'attracteur (A) défini à partir du code fractal W associé à l'image initiale I_{orig} , et pour chaque point (x,y) du document initial, on détermine l'information numérique secondaire à cacher ($I_{in\Omega}$) à partir de ladite différence GAP entre le document initial I_{orig} (donnée) et le document de référence I_{ref} (calculé).

- pour déterminer l'information numérique secondaire à cacher ($I_{in\Omega}$), on établit un lien binaire par convention entre GAP et l'information numérique à cacher $I_{in\Gamma}$. Ainsi, s'il y a correspondance d'après le critère utilisé pour un point donné (x,y) du document, on aura $I_{in\Omega} = GAP$ pour ce pixel; dans le cas contraire, on ne tient pas compte de l'information à cacher pour ce pixel.

- dans un exemple de réalisation, le lien binaire est établi selon la règle suivante:

Si $GAP(x,y) < 0$ et $I_{in\Gamma}(x,y) = 0$ ou $GAP(x,y) > 0$ et $I_{in\Gamma}(x,y) = 1$

alors $I_{in\Omega}(x,y) = GAP(x,y)$

sinon $I_{in\Omega}(x,y) = 0$

- pour extraire d'un document numérique (I'_{orig}) présumé porteur d'une information numérique dissimulée selon le procédé ci-dessus, le procédé comporte des étapes consistant à:

- calculer un code d'autosimilarité W' associé à l'image modifiée I'_{orig} en utilisant le même contexte que celui utilisé lors de l'opération d'insertion;

- récupérer l'information $I'_{in\Omega}$ pour chaque pixel à partir de I'_{orig} et de W' en calculant $I'_{in\Omega} = I'_{orig} - A'$.

- tester l'information $I'_{in\Omega}$ récupérée et si $I'_{in\Omega}$ est positive, en déduire que l'information dissimulée est égale à 1, dans le cas contraire, en déduire que l'information dissimulée est égale à 0 pour le pixel considéré, de sorte qu'on extrait l'information numérique dissimulée à partir du document numérique modifié (I'_{orig}).

L'invention sera mieux comprise à la lecture de la description suivante en référence aux dessins ci-annexés, dans lesquels:

- la figure 1 représente une vue schématique des principales étapes de la phase d'insertion d'information dans un document;

- la figure 2 représente une vue schématique des principales étapes du procédé d'extraction d'information à partir d'un document où elle a été préalablement insérée;

5 - la figure 3 représente sur un exemple d'image les étapes d'une transformation locale établissant la correspondance entre une zone « DOMAIN » de l'image en une zone « RANGE » de l'image;

Principe de l'invention:

10

Comme cela va être décrit de manière plus détaillée plus loin, le principe de l'invention repose sur l'utilisation d'autosimilarités (issues de la théorie des fractales) pour introduire dans l'image une information binaire sans s'exposer aux inconvénients des procédés connus de dissimulation d'image.

15

Alors que la notion d'auto-similarité est essentiellement utilisée en traitement d'images à des fins de compression (par exemple en codage fractal), on décrit ici comment cette notion peut être utilisée pour calculer de manière adéquate une image de référence (I_{ref}) pour la phase d'insertion d'une information binaire (par exemple visuelle) dans un document numérique, par exemple une image en niveaux de gris, et pour calculer une image

20

de référence (I'_{ref}) pour la phase d'extraction de l'information préalablement cachée dans le document numérique.

Plus précisément, il est indiqué comment l'insertion d'une part et l'extraction de cette « information additionnelle » d'autre part peuvent être réalisées.

25

Il est également précisé dans quelle mesure cette information sera préservée dans le cas d'une manipulation non « destructive » de l'image.

L'invention n'est pas limitée au domaine des informations binaires dans une image en niveaux de gris, mais sera retenue dans la description détaillée par voie d'exemple.

30

L'extension de cette approche pour dissimuler des informations autres que binaires d'une part, et sur des supports autres que des images fixes en niveaux de gris d'autre part, est également évoquée plus loin.

L'autosimilarité implique de décrire une image non plus en termes de « pixels » associés à un niveau de gris mais sous la forme : telle zone est « similaire » à telle autre

modulo une transformation donnée.

Nous appellerons dans la suite de ce document « contexte » le choix d'un certain nombre de primitives de découpage de l'image, la manière de les disposer, le critère d'appariement (c'est-à-dire la distance entre l'image de référence I_{ref} et l'image initiale I_{orig}), ainsi que l'ensemble des transformations autorisées entre primitives.

L'image initiale à traiter, que nous appellerons I_{orig} , est découpée en un ensemble de primitives, que l'on appellera « range » ou Cible, qui doivent couvrir la totalité de l'image (avec éventuellement un recouvrement). D'autre part, un dictionnaire de base D_{base} , constitué de primitives « domain » ou Source, est construit. Les éléments de ce dictionnaire sont également (par défaut) extraits de l'image elle-même, mais n'ont pas besoin de couvrir toute l'image à traiter. Il n'y a pas de contrainte particulière sur la répartition des primitives « domain ». Le dictionnaire ainsi construit, est ensuite enrichi en utilisant des transformations géométriques et photométriques pour former un dictionnaire final D_{final} de transformations autorisées. A noter que des éléments peuvent être ajoutés dans le dictionnaire D_{final} , tenus secrets vis-à-vis d'utilisateurs externes, et connus uniquement du logiciel d'insertion/extraction d'information.

Typiquement on utilisera des transformations de type affine pour créer de nouvelles primitives (mais d'autres transformations plus complexes peuvent également être utilisées).

Les transformations peuvent inclure des opérations géométriques (telles qu'une isométrie (i.e. symétries, rotations, réflexions), ou des transformations photométriques, par exemple sur les valeurs de luminance. En particulier, le contexte permettra de définir si des codes contractifs (définis plus loin) sont utilisés.

Il est à noter que pour la mise en oeuvre du procédé par l'intermédiaire d'un logiciel, le contexte défini est déclaré au logiciel chargé d'exécuter les calculs relatifs à l'insertion/extraction d'information dissimulée.

Il s'agit ensuite d'apparier chacune des primitives « range » avec une primitive « domain » du dictionnaire (voir illustration ci-dessous) selon un critère de distance, par exemple la distance minimum. A l'inverse, on peut avoir intérêt dans certains cas à éloigner l'image de référence I_{ref} de l'image initiale I_{orig} , afin de cacher (potentiellement) plus d'information dans la distance entre les deux images, pixel à pixel. On utilisera usuellement la distance euclidienne, mais d'autres distances peuvent être utilisées.

En indexant par i les primitives « range », nous noterons w_i la transformation qui lui

est associée (i.e : la transformation qui définit un élément du dictionnaire de base, plus une transformation). Nous appellerons W , l'union des transformations locales w_i , W l'image composée de l'ensemble des primitives « range » représentées approximativement à partir d'un élément de D_{final} , et A l'attracteur associé à W s'il existe. On rappelle à cet égard que si le code choisi est contractif, il est possible, en utilisant le théorème du collage, de considérer l'attracteur A (c'est-à-dire l'image obtenue en itérant n fois la transformation W à partir de n'importe quelle image initiale I_{init} : $A = W^n(I_{\text{init}})$), à la place de la transformation W , qui est la réunion des blocs « range » approximés à partir de I_{orig} : W est la transformée de I_{orig} par la transformation W appliquée une fois: $W I = W(I_{\text{orig}})$.

Il est rappelé qu'une transformation W donnée définit son attracteur A , puisque la transformation W appliquée n fois à une image quelconque donne l'image A .

Illustration: dans un exemple de mise en oeuvre de l'invention, le contexte (tel que défini plus haut) est ici celui classiquement utilisé en compression d'image: les primitives sont des blocs carrés : de taille 8×8 pixels pour les « range », et 16×16 pixels pour les «domain ». Les transformations autorisées des domaines sont: le sous-échantillonnage par 2 ; la rotation à 0° (c'est-à-dire l'identité), 90° , 180° , 270° ; les symétries en ce qui concerne les transformations géométriques; et un décalage et mise à l'échelle sur les valeurs de luminance.

En d'autres termes, chaque transformation locale w_i peut s'écrire sous la forme:

$$w_i \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_i & b_i & 0 & x \\ c_i & d_i & 0 & y \\ 0 & 0 & S_i & z \end{pmatrix} + \begin{pmatrix} u_i \\ v_i \\ O_i \end{pmatrix}$$

où a_i, b_i, c_i, d_i représentent la transformation géométrique (sous/sur-échantillonnage, plus rotation/réflexion, ...) ; (x,y) représentent les coordonnées du point de l'image et z le niveau de gris associé ; (u_i,v_i) représente le déplacement nécessaire pour mettre en correspondance la position de la primitive « domain » avec la primitive « range » concernée ; s_i et o_i représentent respectivement la mise à l'échelle et le décalage sur les valeurs de luminance.

Visibilité: afin d'assurer l'invisibilité de l'information rajoutée dans l'image originale

et de ne pas dégrader l'image support elle-même (nous l'appellerons dans la suite de ce document I_{orig}), l'invention prévoit de ne pas exposer le problème sous sa forme classique, à savoir: comment ajouter une information sans quelle soit visible, mais plutôt d'exprimer le problème sous un angle nouveau, à savoir: comment décomposer l'image originale I_{orig} en

5 une somme de deux images: une première image (I_{ref}) calculée et essentiellement liée à l'image originale, notée I_{orig} ; et une seconde image, notée I_{inf2} , essentiellement liée à l'information à dissimuler, notée I_{inf1} .

Nous noterons la première image $I_{ref} = WI_{orig}$ (ou A , si W est contractif, ce qui sera l'hypothèse retenue pour la suite) et la seconde I_{inf2} . L'objectif étant que la somme des

10 images $A + I_{inf2}$ (soit l'image modifiée I'_{orig}) soit aussi proche que possible de l'image initiale I_{orig} . Plus précisément, par la proximité de I'_{orig} par rapport à I_{orig} , on exprime le fait que l'image I'_{orig} modifiée par insertion d'une information numérique sera comprise, pixel à pixel, dans un intervalle borné d'une part par l'image initiale I_{orig} , qui est donnée, et d'autre part par l'image de référence I_{ref} , qui est calculée, le mode de calcul étant défini à

15 partir du contexte (défini plus haut) La luminance de chaque pixel de I'_{orig} sera donc comprise entre (ou égale à, ou reprérée par) sa valeur dans I_{ref} et sa valeur dans I_{orig} .

Description de l'insertion d'une information dans une image:

On se réfère à la figure 1, dans laquelle les blocs à coins carrés indiquent des

20 données, et les blocs à coins arrondis indiquent des opérations effectuées sur les données. On constate que l'image modifiée I'_{orig} est obtenue par addition d'une part du document de référence I_{ref} , ou, en cas d'utilisation des fractales, l'attracteur A , et d'autre part, de I_{inf2} , elle-même obtenue à partir de l'information à dissimuler I_{inf1} , et de la différence point à point (notée GAP), entre le document original I_{orig} , et le document de référence (I_{ref} ; A).

25 On va maintenant décrire la détermination de l'image de référence I_{ref} (soit A dans le cas d'un code contractif utilisant les autosimilarités de l'image à partir de l'image d'origine I_{orig} , et, d'autre part, la détermination de l'information I_{inf2} à partir de l'information à cacher I_{inf1} , ces déterminations étant telles que $A + I_{inf2} = I'_{orig}$, suffisamment proche de l'image d'origine I_{orig} pour que le document d'origine ne soit pas dégradé visuellement: I'_{orig} doit

30 apparaître comme I_{orig} .

Détermination de I_{ref} (A) à partir de I_{orig} :

On se réfère aux figures 1 et 3.

Pour déterminer le document numérique de référence (I_{ref}) à partir du document initial (I_{orig}), on utilise la méthode des fractales, consistant à:

- découper le document initial (I_{orig}) en un ensemble de primitives $RANGE(i)$ couvrant la totalité du document initial;
- extraire du document initial (I_{orig}) un ensemble de primitives $DOMAIN(i)$, de façon à constituer un dictionnaire de primitives $DOMAIN(i)$ de base (D_{base});
- à partir du dictionnaire de primitives $DOMAIN$ de base, déterminer un dictionnaire (D_{final}) de primitives $DOMAIN$ supplémentaires, en appliquant aux primitives de base, un ensemble de transformations géométriques et/ou photométriques locales w_i ; de plus, il est envisageable d'inclure dans D_{final} des éléments secrets pour renforcer la sécurité.
- appairer chacune des primitives de base $RANGE(i)$ avec une primitive $DOMAIN(i)$ des dictionnaires de primitives (D_{final}), de telle manière que chaque primitive $RANGE(i)$ soit égale à la transformée d'une primitive $DOMAIN(i)$ par une transformation locale w_i , plus une erreur (ϵ_i) permettant de dissimuler l'information numérique à cacher (I_{inf}), l'image composée de l'ensemble des primitives $RANGE$ remplacées par un élément du dictionnaire (D_{final}) étant l'image de référence, notée A .

On se fixe un contexte, tel que défini plus haut. Le contexte doit être choisi en fonction des critères suivants:

- la robustesse recherchée : les transformations géométriques autorisées entre blocs « domain » et « range » permettront ensuite de « sauvegarder » l'information ajoutée si l'on opère ces mêmes transformations (bien ou malveillantes) sur l'image modifiée. La contrainte principale réside dans le fait qu'il sera indispensable d'utiliser le même contexte cohérent lors de l'extraction de l'information ajoutée, que celui utilisé pour la procédure d'insertion.
- l'éloignement (et positionnement) entre I_{orig} et A recherché : plus A sera numériquement éloigné, c'est-à-dire différent de I_{orig} , plus la place pour cacher une information supplémentaire sera importante, mais les risques de visibilité de l'insertion d'information dans l'image d'origine augmenteront.
- la « stabilité du code » (en l'absence de manipulations parasites): c'est à dire assurer que A' sera « proche » de A , puisque les deux images I_{orig} et I'_{orig} sont « similaires ».

Détermination de I_{inf2} à partir de l'information à dissimuler I_{inf1}

Soit I_{inf0} l'information binaire initiale que l'on souhaite ajouter dans l'image originale; le contenu de I_{inf0} dépendra pour beaucoup de l'utilisation visée par ce procédé d'insertion/extraction. Si I_{inf0} et I_{orig} ne sont pas de la même taille, alors I_{inf0} doit être transformée en une image I_{inf1} de taille identique à I_{orig} . On considérera donc que l'information réelle à dissimuler dans l'image I_{orig} est I_{inf1} . Le passage de l'information à dissimuler I_{inf0} à une information à dissimuler I_{inf1} mise en forme est représentée dans la figure 1 par une étape notée (0).

On définit alors une grandeur I_{inf2} , qui est en réalité l'image de l'information I_{inf1} « modulée » en fonction de la valeur du GAP entre l'image d'origine I_{orig} et l'image de référence calculée I_{ref} . I_{inf2} sera défini à partir de I_{inf1} de la manière suivante:

A l'étape notée (1), on calcule la différence des images I_{orig} et $I_{ref} = A$, notée GAP:

$GAP = I_{orig} - I_{ref}$, soit $I_{orig} - A$ pour un code contractif;

- on choisit un critère de correspondance entre GAP et l'information à cacher I_{inf1} . A titre d'exemple, on retiendra comme critère la solution suivante, qui n'est nullement limitative:

si $(GAP(x,y) < 0 \text{ et } I_{inf1}(x,y) = 0)$ Ou $(GAP(x,y) > 0 \text{ et } I_{inf1}(X,Y) = 1)$

alors $I_{inf2}(x,y) = GAP(x,y)$

sinon $I_{inf2}(X,Y) = 0$

Ce critère de correspondance entre GAP et I_{inf1} permet d'établir un lien binaire entre GAP qui est codé par son signe (positif ou négatif), et l'information numérique à cacher au pixel considéré, qui vaut 1 ou 0. On peut introduire différentes variantes sur cette façon de moduler I_{inf2} entre 0 et la valeur du GAP, en prenant d'autres valeurs de bornes, par exemple 1 et 1,2 fois la valeur de GAP, au lieu de 0 et une fois la valeur de GAP.

Remarque: du fait de cette convention, il est à noter qu'en moyenne, seul un point sur deux (au moins) de l'information à ajouter I_{inf1} sera réellement pris en compte. Il est possible de le garantir en inversant si besoin est l'information binaire à insérer.

Il faut néanmoins relativiser cette première remarque d'un point sur deux. En effet,

nous pouvons considérer une image intermédiaire I_{mid} où chaque point serait la valeur moyenne de I_{orig} et I_{ref} ; puis modifier le critère de correspondance afin de construire I_{inf2} comme suit : $I_{inf2}(X,Y) = +GAP/2$ si $(GAP(x,y) < 0$ et $I_{inf1}(x,y) = 0$) ou $(GAP(x,y) > 0$ et $I_{inf1}(X,Y) = 1)$ ou, $-GAP/2$ sinon. Ainsi chaque point de I'_{orig} sera porteur d'une information de I_{inf1} . Cependant, en contrepartie, la « force » d'insertion sera divisée par un facteur 2 par rapport à la convention précédemment proposée. Enfin, il sera évidemment nécessaire de modifier en conséquence les conventions utilisées lors de la phase d'extraction.

Notons également que le critère de construction de I_{inf2} peut être facilement modifié pour faire en sorte que l'image I'_{orig} soit la « plus proche possible » de I_{ori} . Néanmoins, il y a là un compromis à faire entre visibilité de l'insertion et nombre de points de l'information binaire à insérer, réellement pris en compte (et dans quelle proportion). Ce compromis est à définir en fonction de l'utilisation visée par le procédé de dissimulation. On peut par exemple, décider de forcer à GAP tous points associé à une différence (GAP) supérieure à un certain seuil en valeur absolue, ou bien encore fixer en fonction d'un bon équilibre local que des points de I'_{orig} soient affectés (même si le critère de correspondance n'est pas vérifié) à la valeur de I_{orig} , de façon à éviter les concentrations de zones en moyenne trop proches de I_{ref} ; mais dans ce cas, ces même points ne pourront plus être porteurs d'information dissimulée.

La visibilité du procédé d'insertion sera fonction de $(I_{orig} - I'_{orig})$: la visibilité sera d'autant plus grande que la différence entre l'image d'origine et l'image modifiée par insertion sera élevée.

On va maintenant décrire le procédé d'extraction de l'information cachée I'_{inf2} à partir d'une image modifiée I'_{orig} . Pour cela, on se réfère à la figure 2.

De manière duale à l'insertion, l'extraction sera réalisée de la manière suivante, tel que schématisé en figure 2.

- Calcul du code d'auto-similarité W' associé à I'_{orig} en utilisant le même contexte que celui utilisé lors de l'opération d'insertion; ceci donne dans l'étape indiquée (1'), un document de référence, noté I'_{ref} dans le cas général, ou A' en cas de calcul de I'_{ref} par méthode fractale.

- Récupération de I'_{inf2} à partir de I'_{orig} et de A' , de la manière suivante:

$$I'_{inf2} = I'_{orig} - A'$$

Il est à noter que A' est à I'_{orig} ce qu'était A à I_{orig} dans la phase d'insertion

d'information dans I_{orig} . Donc on essaie de reconstruire une image de référence A' à partir de l'image modifiée I'_{orig} .

Notons que d'une part, les codes IFS associés aux images I_{orig} et A sont identiques (le premier par construction, et le second par définition d'un attracteur), et d'autre part, chaque point-image de I_{orig} est inclus dans l'intervalle défini par sa valeur dans I_{orig} et dans A .

Détermination de l'information cachée I'_{inf1} , à partir de I'_{inf2} :

I'_{inf1} peut se calculer à partir de I'_{inf2} de la manière suivante: de manière duale par rapport à l'opération d'insertion, le test utilisé est le suivant:

si $I'_{inf2}(x,y) > \text{seuil prédéterminé}$, alors $I'_{inf1}(x,y) = 1$

sinon si $I'_{inf2}(x,y) < \text{seuil}$ alors $I'_{inf1}(x,y) = 0$

sinon « on ne sait pas dire » (car le pixel (x,y) ne contient pas d'information cachée)

Par défaut, le seuil prédéterminé est fixé à 0, mais comme indiqué pour l'étape d'insertion d'information, on peut utiliser d'autres seuils « plus larges » afin de limiter les risques de se tromper en chaque point (x,y) ; mais dans ce cas on diminue d'autant le nombre d'informations binaires récupérées sur l'ensemble de ce que l'on a dissimulé. Le seuil est à régler en fonction de la modulation adoptée pour l'insertion. Ces réglages du paramétrage relèvent du savoir-faire de l'homme de métier, ou bien de l'application.

AVANTAGES DE L'INVENTION:

L'invention telle qu'elle vient d'être décrite répond aux buts fixés, présente plusieurs avantages par rapport aux procédés connus, et notamment:

Robustesse vis à vis de manipulations bien/malveillantes:

Considérons maintenant que l'image sur laquelle on souhaite récupérer l'information cachée ne soit plus, l'orig mais I'_{orig} , suite à une manipulation bien ou malveillante.

Grâce à l'utilisation des autosimilarités de l'image et des fractales, l'information extraite est « stable » si l'on opère des manipulations géométriques et/ou photométriques

précédemment « autorisées » lors de la recherche des similarités entre primitives « range » et « domain » (i.e. incluses dans le contexte). En d'autres termes, il sera possible de dissimuler une information dans une image, puis de faire subir des transformations autorisées (faisant partie du dictionnaire D_{final}) à l'image modifiée, tout en restant capable d'extraire à nouveau l'information dissimulée à partir de l'image transformée. Il est important de considérer que pour augmenter la robustesse du procédé selon l'information, il suffit de définir un plus grand nombre de transformations autorisées dans le contexte. Des exemples de transformations classiques de l'image sont citées ci-dessous.

10 Transformations photométriques.

Si l'image I_{orig} est modifiée en une image I''_{orig} , telle que pour chaque primitive « domain » l'on ait $I''_{orig} = \alpha I'_{orig} + \beta$ alors $J''_{in\Omega} = I'_{in\Omega}$, signifiant que l'insertion d'information résiste à des transformations photométrique affines.

15

Transformations géométriques.

Si l'on utilise le contexte décrit précédemment, en cas de rotation à 0° , 90° , 180° , 270° degrés $I'_{in\Omega}$ subira la même modification R que l'image I' elle-même (i.e. $I'_{in\Omega} = R(I'_{in\Omega})$). En cas de changement d'échelle H , nous aurons: $I''_{in\Omega} = H(I'_{in\Omega})$.

20

En cas de décalage (i.e.: translation),... les parties de l'image éventuellement supprimées entraîneront la suppression de $I'_{in\Omega}$ pour les mêmes zones, mais le reste de l'information dissimulée demeurera dans son ensemble.

Plus généralement, il suffit que:

$$\text{signe} \{Tf(I''_{in\Omega}(x,y))\} = \text{signe} (I'_{in\Omega}(x,y))$$

$$\text{pour garantir que } I''_{in\Omega}(x,y) = I'_{in\Omega}(x,y).$$

25

où $\text{signe}(X) = 0$ si $X=0$; $+1$ si $X>0$ et -1 si $X<0$; et Tf est défini par:

$$I''_{orig} = Tf\{I'_{orig}\}$$

La prise en compte du signe de l'information rajoutée pendant une transformation plutôt que la valeur exacte du GAP entraîne plus de robustesse, puisqu'on a enfoui dans l'image une information plus importante que celle dont on a réellement besoin pour l'extraction de $I_{in\Omega}$.

30

EXTENSIONS DE L'INVENTION

L'invention telle que décrite plus haut en termes généraux peut aisément être étendue et appliquée à des situations spécifiques, comme indiqué dans les exemples ci-dessous.

Par exemple, le principe de l'invention peut être adapté aux Images en couleurs.

- 5 Selon le système de couleurs utilisé, il sera éventuellement nécessaire d'opérer un changement de repère pour passer dans un repère de type Luminance/chrominance (ou également sous la forme: luminance, teinte, saturation). Cette opération est inversible ; dans le cas d'images RVB (Rouge Vert Bleu), il faudra donc passer en Luminance/Chrominance, puis réaliser l'opération d'insertion, et enfin réaliser l'opération inverse pour revenir en RVB.
- 10 Une fois la composante de luminance isolée, les opérations d'insertion et d'extraction peuvent se réaliser exactement comme décrit précédemment dans le cas des images en niveaux de gris.

Notons, que l'information ajoutée restera présente lors d'une conversion d'une image couleur l'orig en une image I''_{orig} en niveaux de gris.

- 15 Egalement, le principe de l'invention peut être adapté aux images Vidéo. Deux possibilités existent: soit opérer image par image, et ce en insérant l'information additionnelle de la manière décrite précédemment pour les images fixes, soit étendre l'approche utilisée pour estimer le code IFS en utilisant une primitive spatio-temporelle au lieu d'une primitive spatiale (typiquement, des cubes plutôt que des blocs carrés). Notons
- 20 qu'une vidéo comporte bien évidemment potentiellement beaucoup plus de place pour d'une part, dissimuler plus d'informations et d'autre part, la dissimuler de manière plus robuste en augmentant la redondance.

En outre, le principe de l'invention peut être adapté à l'insertion d'une information autre que binaire.

- 25 Il est par ailleurs envisageable d'insérer une information autre que binaire à l'aide de la technique des plans de bits : l'information en niveaux de gris sera classiquement décomposée comme une somme pondérée (par puissance de 2) d'images binaires. Dans le cas, d'une information $I_{\text{inf } 0 \text{ sur } 255 \text{ niveaux de gris}}$ de taille $k \times k$, l'information binaire à insérer sera donc de taille $8k \times 8k$. Si la place réservée à l'information à cacher est suffisante,
- 30 le principe peut également être étendu à des informations couleurs.

Enfin, l'invention peut être adaptée à la dissimulation de signaux audio numérisés, dans un document, ou inversement.

APPLICATIONS INDUSTRIELLES DE L'INVENTION:

De nombreuses utilisations de ce procédé sont d'ores et déjà envisageables : la signature, l'intégrité, la non-répudiation, la traçabilité, voire la correction d'erreurs, et les points de contrôle de réseau. Selon l'utilisation visée, le procédé présenté peut être utilisé tel quel, modulo la définition d'un contexte adéquat; de définir le type d'information à dissimuler (i.e. : le « design » de la marque), ainsi que le paramétrage des opérateurs d'insertion et extraction. Des exemples d'application sont donnés ci-dessous à titre indicatif.

10 **Signature.** Il s'agit pour un auteur, une société ou autre de protéger un document tel qu'une image. Cela peut se faire en insérant comme information binaire le logo de la société ou bien par exemple le visage de l'auteur.

15 **Intégrité.** Il s'agit ici de pouvoir identifier si une image a été sensiblement modifiée ou non. Pour cela, l'information à dissimuler sera liée aux caractéristiques de l'image elle-même: histogramme des niveaux de gris (sous forme d'image binaire), carte des contours (en superposition de l'image), ou encore un motif spécifique... Notons néanmoins la difficulté suivante : les caractéristiques d'une image seront modifiées par le fait même de dissimuler dans l'image elle-même ses caractéristiques.

20 **Non-répudiation.** Il s'agit ici d'insérer automatiquement une trace de l'auteur lorsque celui-ci envoie une image vers une tierce personne : un logo identifiant la personne (empreinte digitale, signature numérique,...) et/ou, la machine à partir de laquelle celui-ci transmet l'image (fax, PC, terminal mobile Multimédia,...).

25 **Traçabilité.** L'utilisation peut être étendue ou automatisée de telle sorte que l'on sache par exemple à l'aide d'une trace si telle ou telle image a été ou non précédemment photocopiée, imprimée,...

Point de contrôle de réseau:: l'invention pourra être utilisée pour éviter que des images interdites transitent sur des réseaux (comme Internet) en profitant de transformations simples effectuées juste avant des points de contrôle automatiques implantés sur le réseau, et effectuées en sens inverse juste après

30 D'autres utilisations comme la correction d'erreurs peuvent également être envisagées. Le principe consisterait à insérer dans les zones d'images considérées comme peu importantes, des informations sur la ou les zones considérées elles comme très

importantes. En cas de perte partielle/totale des zones importantes, une récupération partielle de celles-ci serait alors possible à partir de l'information dissimulée dans les zones initialement considérées comme peu importantes.

REVENDEICATIONS

1. Procédé pour dissimuler une information numérique primaire (I_{in1}) dans un document numérique initial, notamment un document multimedia initial (I_{orig}), caractérisé en ce qu'il comporte des étapes consistant à:

- décomposer le document initial (I_{orig}) à priori, en déterminant un document numérique de référence (I_{ref}) fonction du document numérique initial (I_{orig}), et une information numérique secondaire (I_{in2}) fonction de l'information numérique primaire à cacher (I_{in1}), tels que la somme du document numérique de référence (I_{ref}) et de ladite information numérique secondaire (I_{in2}) soit un document modifié (I'_{orig}) sensiblement égale au document numérique initial (I_{orig});

- insérer l'information numérique secondaire (I_{in2}) ainsi déterminée dans ledit document initial, en calculant une image modifiée (I'_{orig}) constituée par la somme dudit document numérique de référence (I_{ref}) et de ladite information numérique secondaire (I_{in2}), de façon à obtenir un document numérique modifié (I'_{orig}) proche du document initial (I_{orig}) mais intégrant de façon sensiblement indiscernable l'information numérique primaire (I_{in1}) à dissimuler.

2. Procédé selon la revendication 1, caractérisé en ce que la valeur de chaque pixel du document modifié (I'_{orig}) est comprise entre sa valeur dans le document numérique de référence (I_{ref}) et sa valeur dans le document initial (I_{orig});

3. Procédé selon la revendication 1 ou la revendication 2, caractérisé en ce que pour déterminer le document numérique de référence (I_{ref}) à partir du document initial (I_{orig}), on utilise la méthode des fractales, consistant à:

- découper le document initial (I_{orig}) en un ensemble de primitives RANGE(i) couvrant la totalité du document initial;

- extraire du document initial (I_{orig}) un ensemble de primitives DOMAIN(i), de façon à constituer un dictionnaire de primitives DOMAIN(i) de base (Dbase);

- à partir du dictionnaire de primitives DOMAIN de base, déterminer un dictionnaire (Dfinal) de primitives DOMAIN supplémentaires, en appliquant aux primitives de base, un

ensemble de transformations géométriques et/ou photométriques locales W_i ;

- appairer chacune des primitives de base $RANGE(i)$ avec un élément du dictionnaire (D_{final}), de telle manière que chaque primitive $RANGE(i)$ soit égale à la transformée d'une primitive $DOMAIN(j)$ par une transformation locale w_i , plus une erreur (ϵ_i) permettant de
5 dissimuler l'information numérique à cacher ($I_{in\Omega}$), l'image composée de l'ensemble des primitives $RANGE$ approximées à partir d'une primitive $DOMAIN$ constituant l'image de référence, notée I_{ref} .

4. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce que pour déterminer
10 l'information numérique secondaire à cacher ($I_{in\Omega}$) à partir de l'information numérique primaire à cacher ($I_{in\Omega}$), on calcule la différence $GAP = I_{orig} - A$ entre le document initial (I_{orig}) et l'attracteur (A) défini à partir du code fractal (W) associé au document initial (I_{orig}), et pour chaque point (x,y) du document initial, on détermine l'information numérique secondaire à cacher ($I_{in\Omega}$) à partir de ladite différence GAP et de l'information primaire à
15 cacher;

- pour déterminer l'information numérique secondaire à cacher ($I_{in\Omega}$), on établit un critère de lien binaire par convention entre GAP et l'information numérique à cacher $I_{in\Omega}$, et s'il y a correspondance d'après le critère utilisé pour un point donné (x,y) du document, on aura $I_{in\Omega} = GAP$ pour ce pixel; dans le cas contraire, on ne tient pas compte de l'information
20 à cacher pour ce pixel.

5. Procédé selon la revendication 4, caractérisé en ce que le lien binaire est établi selon la règle suivante:

Si $GAP(x,y) < 0$ et $I_{in\Omega}(x,y) = 0$ ou $GAP(x,y) > 0$ et $I_{in\Omega}(x,y) = 1$
25 alors $I_{in\Omega}(x,y) = GAP(x,y)$
sinon $I_{in\Omega}(x,y) = 0$

6. Procédé pour extraire d'un document numérique I'_{orig} présumé porteur d'une information numérique dissimulée selon le procédé de la revendication 1, caractérisé en ce
30 que l'extraction de l'information dissimulée $I'_{in\Omega}$ comporte des étapes consistant à:

- calculer un code d'autosimilarité W' associé à I'_{orig} en utilisant le même contexte que celui utilisé lors de l'opération d'insertion;

- récupérer l'information dissimulée $I'_{in\Omega}$ à partir de I'_{orig} et de A' en calculant $I'_{in\Omega} = I'_{orig} - A'$;

- tester l'information $I'_{in\Omega}$ récupérée, et si elle est positive, en déduire que l'information dissimulée est supérieure ou égale à 1, dans le cas contraire, en déduire que l'information dissimulée $I'_{in\Omega}$ est égale à 0 pour le pixel considéré, de sorte qu'on extrait l'information numérique dissimulée à partir du document numérique modifié I'_{orig} .

7. Procédé selon la revendication 6, caractérisé en ce que pour tester l'information $I'_{in\Omega}$.

10 - à partir de l'information $I'_{in\Omega}$ récupérée, calculer l'information initialement dissimulée $I'_{in\Omega}$, en appliquant la règle suivante:

si l'information récupérée $I'_{in\Omega}(x,y)$ est supérieur à un seuil prédéterminé S , alors l'information dissimulée $I'_{in\Omega}(x,y) = 1$

sinon si l'information récupérée $I'_{in\Omega}(x,y)$ est inférieure au seuil $(-S)$,

15 alors $I'_{in\Omega}(x,y) = 0$

sinon, en déduire que l'information récupérée $I'_{in\Omega}$ au point (x,y) ne porte pas d'information dissimulée.

1/3

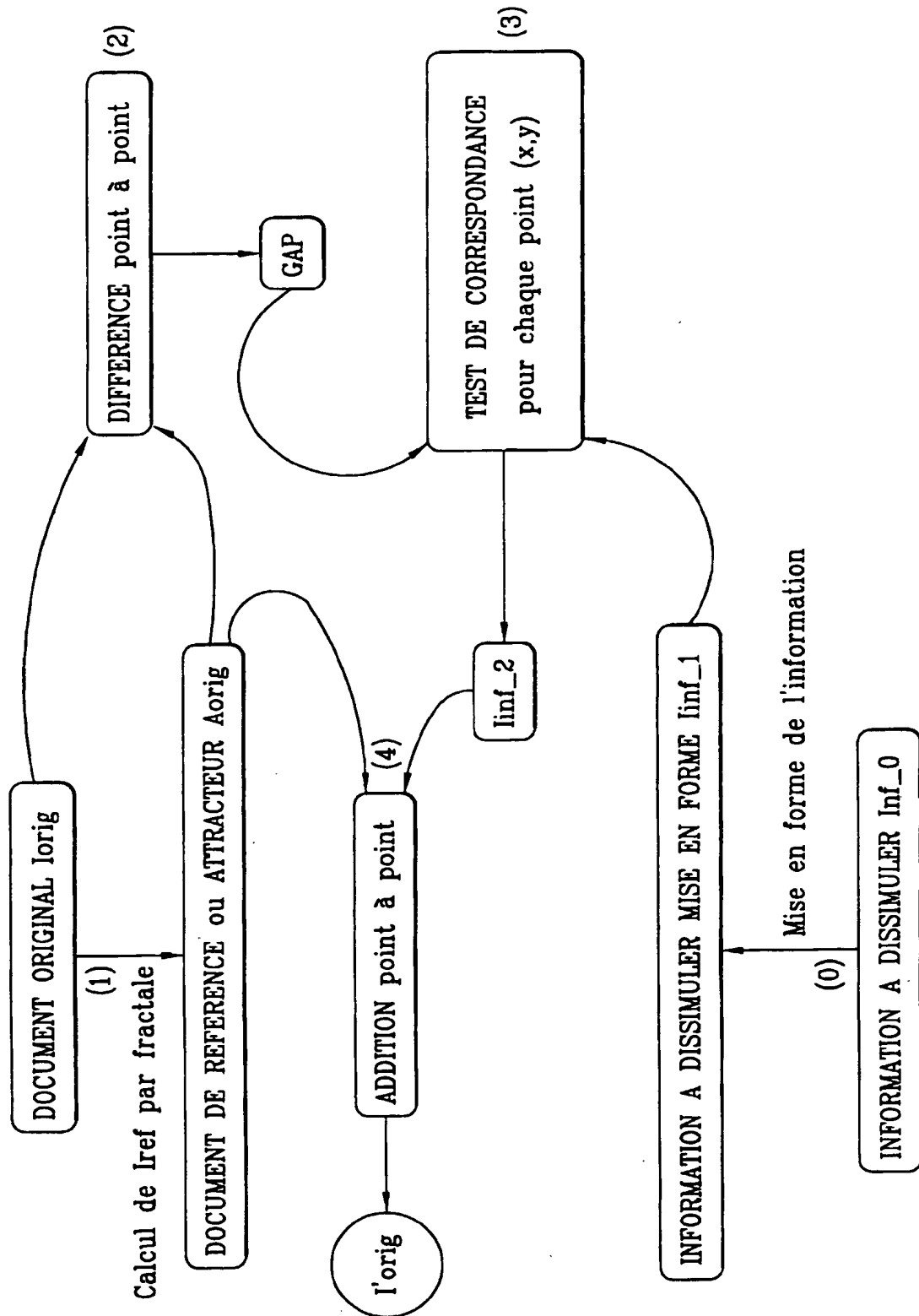
FIG.1

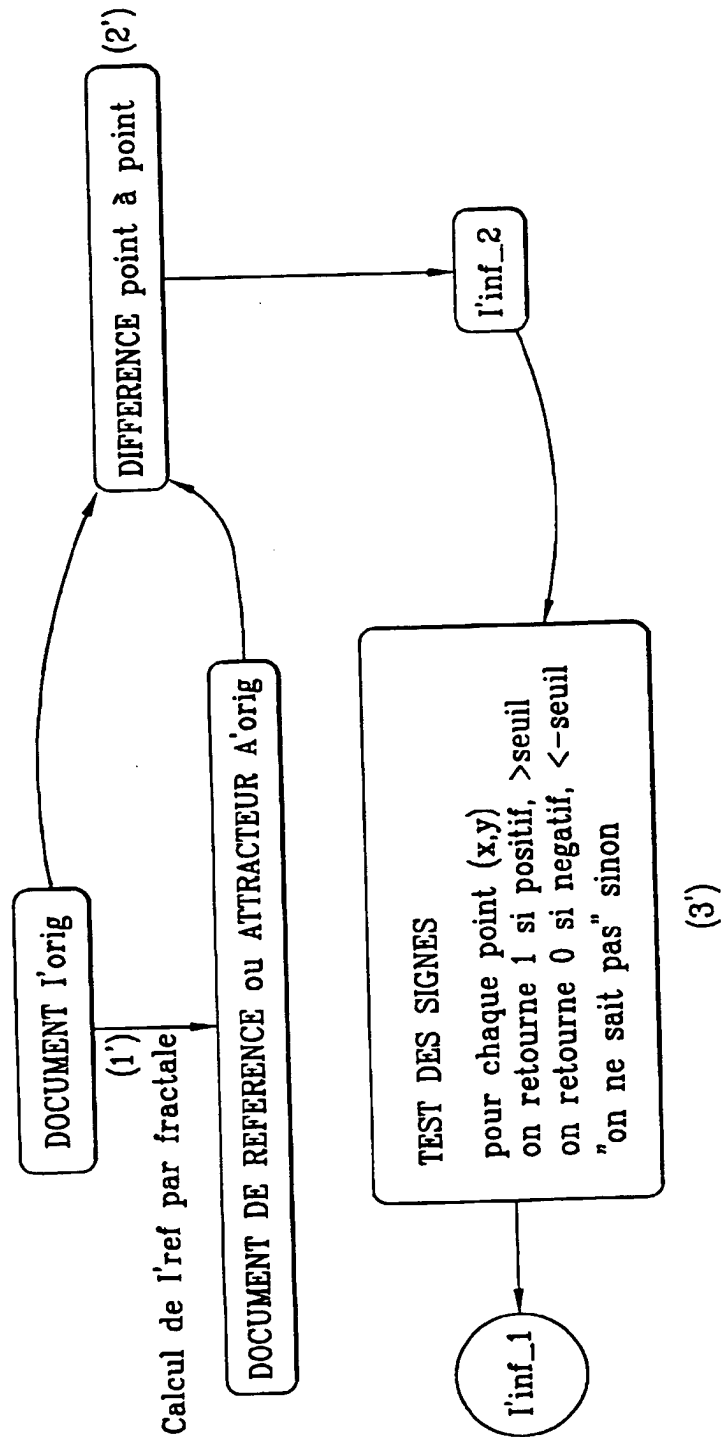
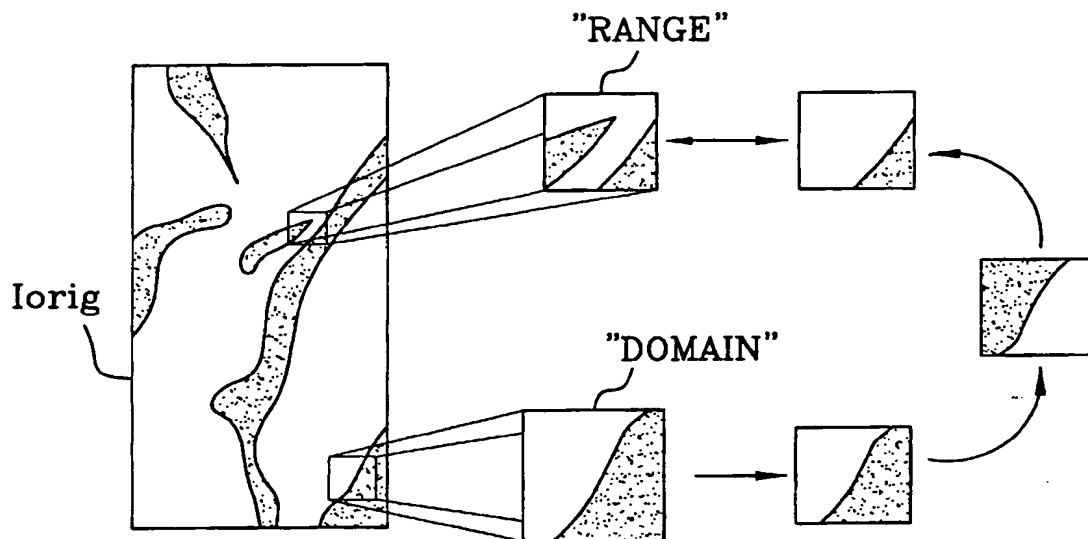
FIG.2

FIG.3

2775812

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIÉTÉ INDUSTRIELLE

**RAPPORT DE RECHERCHE
PRELIMINAIRE**

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 558604
FR 9804083

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	DAVERN P ET AL: "FRACTAL BASED IMAGE STEGANOGRAPHY" INFORMATION HIDING. INTERNATIONAL WORKSHOP PROCEEDINGS, 30 mai 1996, pages 279-294, XP002048612 * le document en entier *	1,3-7
A	PUATE JOAN, JORDAN FRED: "Using Fractal Compression Scheme to Embed a Digital Signature into an Image" VIDEO TECHNIQUES AND SOFTWARE FOR FULL-SERVICE NETWORKS, 21 novembre 1996, pages 108-118, XP002085678 * le document en entier *	1,3-7
		DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)
		H04N
Date d'achèvement de la recherche		Examineur
25 novembre 1998		Hubeau, R
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>		

1

EPO FORM 1503 03 92 (P4C13)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 10 0390

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	FR 2 775 812 A (INST EURECOM) 10 September 1999 (1999-09-10) * abstract * * page 2, line 2 - line 8 * * page 2, line 24 - page 3, line 13 * * page 6, line 6 - page 7, line 11 * * page 4, line 20 - line 30 * * page 11, line 22 - page 12, line 6 * * page 15, line 1 - line 29 * * figures 1,2 *	1-8	G06F17/60
X	EP 0 953 938 A (HEWLETT PACKARD CO) 3 November 1999 (1999-11-03) * abstract * * page 2, column 1, line 34 - column 2, line 32 * * page 2, column 2, line 41 - page 3, column 3, line 51 * * page 9, column 16, line 23 - page 10, column 18, line 8 *	1,4,6-8	
X	US 5 465 299 A (MATSUMOTO HIROSHI ET AL) 7 November 1995 (1995-11-07) * column 6, line 7 - column 7, line 42 * * column 12, line 17 - line 55 * * column 8, line 57 - column 9, line 31 * * figures 2A,2B,3,5,12,13 *	1,6	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F
A	WONG P W: "A WATERMARK FOR IMAGE INTEGRITY AND OWNERSHIP VERIFICATION" PROCEEDINGS. IS&T'S PICS CONFERENCE. ANNUAL CONFERENCE, PROCEEDINGS OF CONFERENCE OF THE SOCIETY FOR IMAGING SCIENCE AND TECHNOLOGY, XX, XX, 17 May 1998 (1998-05-17), pages 374-379, XP000964707 * abstract * * section "Introduction" on pages 374-375	1,4,6-8	
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 29 October 2003	Examiner Cirstet, A
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

THIS PAGE BLANK "HISTO"

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 01 10 0390

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-10-2003

Patent document cited in search report			Publication date	Patent family member(s)	Publication date
FR 2775812	A	10-09-1999	FR	2775812 A1	10-09-1999
			EP	0985313 A1	15-03-2000
			WO	9945696 A1	10-09-1999
EP 0953938	A	03-11-1999	US	2001046307 A1	29-11-2001
			EP	0953938 A2	03-11-1999
			JP	11355558 A	24-12-1999
US 5465299	A	07-11-1995	JP	3260524 B2	25-02-2002
			JP	6224896 A	12-08-1994

2

THIS PAGE BLANK (USPTO)